US006788681B1

(12) **United States Patent**
Hurren et al.

(10) **Patent No.: US 6,788,681 B1**
(45) **Date of Patent: Sep. 7, 2004**

(54) **VIRTUAL PRIVATE NETWORKS AND METHODS FOR THEIR OPERATION**

(75) Inventors: **Alan J. Hurren**, Nepean (CA); **Joseph M. Regan**, Sunnyvale, CA (US); **Paul Bottorff**, Palo Alto, CA (US); **Mark Cobbold**, Stittsville (CA)

(73) Assignee: **Nortel Networks Limited**, St. Laurent, Quebec (CA)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/513,244**

(22) Filed: **Feb. 25, 2000**

Related U.S. Application Data

(63) Continuation-in-part of application No. 09/475,042, filed on Dec. 30, 1999, and a continuation-in-part of application No. 09/270,733, filed on Mar. 16, 1999.
(60) Provisional application No. 60/183,049, filed on Dec. 30, 1999.

(51) **Int. Cl.**[7] **H04L 12/56**
(52) **U.S. Cl.** **370/389**; 370/392
(58) **Field of Search** 370/389–395, 370/466, 230, 400, 401, 350, 250, 423, 465; 709/223–227, 230–233, 243–249, 200; 345/629

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,627,052	A		12/1986	Hoare et al.
5,684,800	A		11/1997	Dobbins et al.
5,862,338	A	*	1/1999	Walker et al. 709/224
5,978,378	A		11/1999	Van Seters et al.

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

WO	WO 95 01023	A	1/1995
WO	WO 99 00948	A	1/1999

OTHER PUBLICATIONS

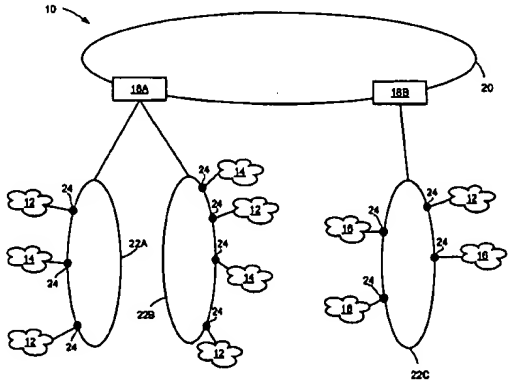
Alan Hurren et al., Transparent LAN Service Network Solution, Jan. 20, 1999, pp. 1–13.
Tom Downey, "Overview of Tag Switching", Electronics Industries Forum of New England, 1997, Professional Program Proceedings Boston, MA, USA May 6–8, 1997, New York, NY, USA, IEEE, US, May 6, 1997 , pp. 61–66, XP010234255, ISBN: 0–7803–3987–8.
Haeryong Lee et al., "End–to–End QoS Arhitecture for VPNs: MPLS VPN Deployment in a Backbone Network", (Aug. 2000), Proceedings of the International Workshops on Parallel Processing, pp. 479–483.

Primary Examiner—Chi Pham
Assistant Examiner—Prenell Jones

(57) **ABSTRACT**

A method and apparatus for providing a Virtual Private Network (VPN) over a connectionless network connecting a plurality of Local Area Networks (LANs), such as an Ethernet network, is disclosed. The method and apparatus comprises associated each VPN with a unique identifier and each LAN of the VPN with a interface device connecting the LAN to the connectionless network, which may be for example, a Synchronous Optical Network (SONET). The interface device may service a plurality of LANs. Accordingly, each LAN is associated with a User-Network Interface that forms part of the interface device. Each data packet destined for a second LAN, such Ethernet frames, received by the interface device for a first LAN is encapsulated with, if known, a Media Access Control (MAC) address of the interface device connected to the second LAN, the VPN's unique identifier, and the port on the interface device connected to the second LAN. Additionally, the corresponding MAC and port address of the first interface device is also used to encapsulate the Ethernet frames. If the MAC and port address is not known (i.e., it is not stored in a database on the first interface device), the first interface device multicasts an encapsulated Ethernet packet to the entire VPN. The first interface device maintains (i.e., updates and appends) its database of MAC and port addresses in response to encapsulated data frames received by the first interface device.

46 Claims, 9 Drawing Sheets



U.S. PATENT DOCUMENTS

6,041,057 A		3/2000	Stone	
6,085,238 A	*	7/2000	Yuasa et al.	709/223
6,151,324 A		11/2000	Belser et al.	
6,173,334 B1	*	1/2001	Matsuzaki et al.	709/245
6,175,571 B1	*	1/2001	Haddock et al.	370/423
6,185,214 B1		2/2001	Schwartz et al.	
6,205,488 B1		3/2001	Casey et al.	
6,414,958 B1		7/2002	Specht	
6,512,766 B2		1/2003	Wilford	
6,526,056 B1	*	2/2003	Rekhter et al.	370/395
6,577,642 B1	*	6/2003	Fijolek et al.	370/465

* cited by examiner

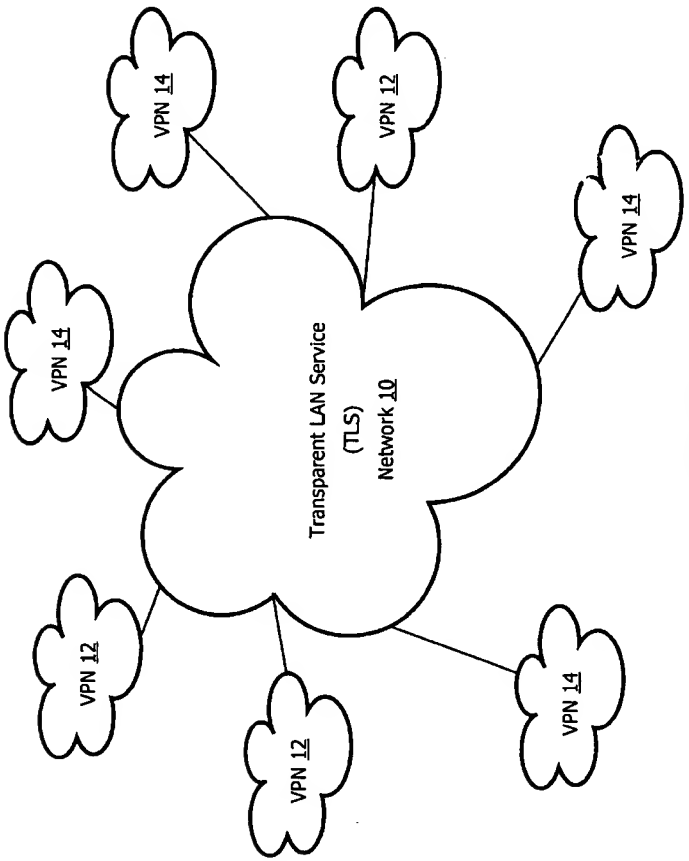


FIGURE 1

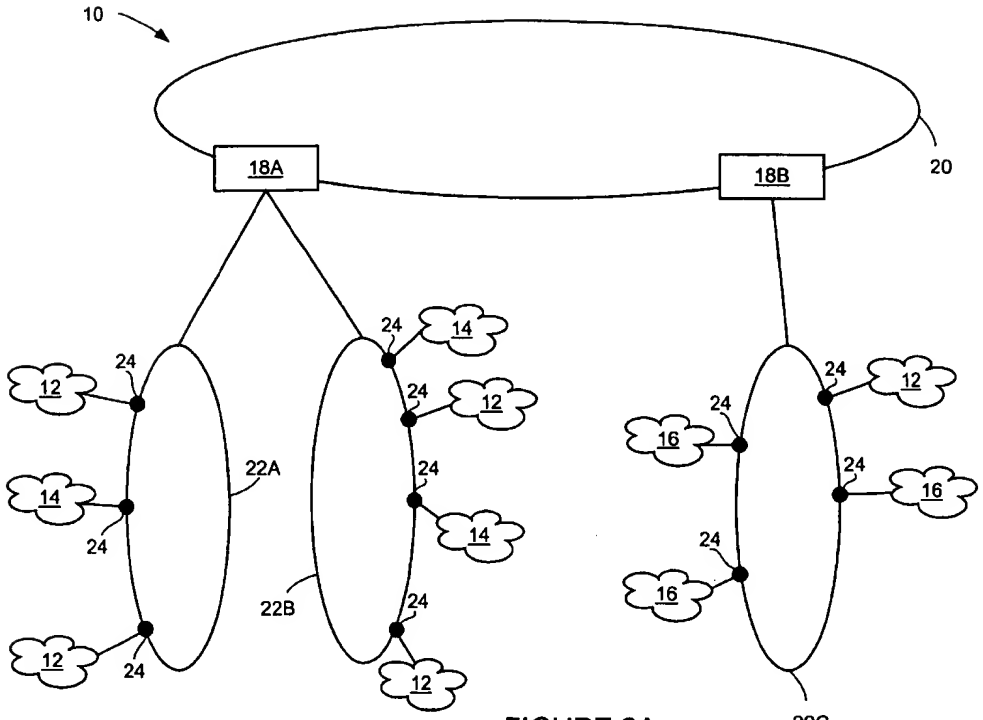


FIGURE 2A

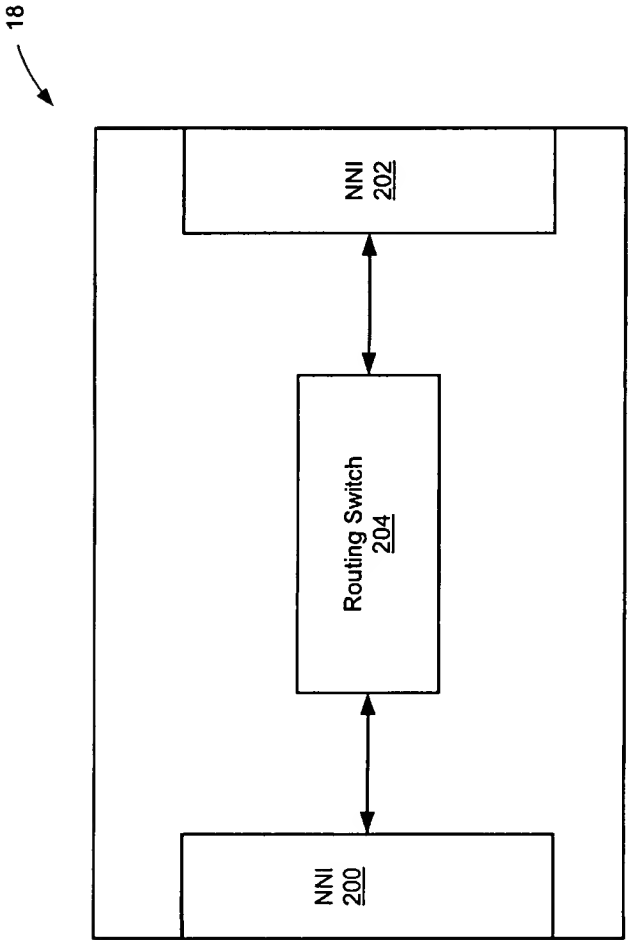


FIGURE 2B

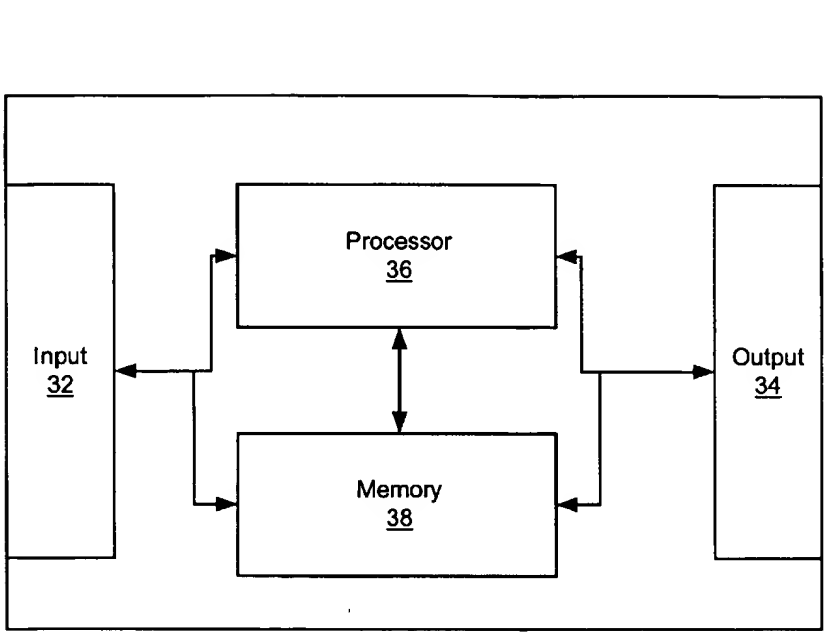


FIGURE 3

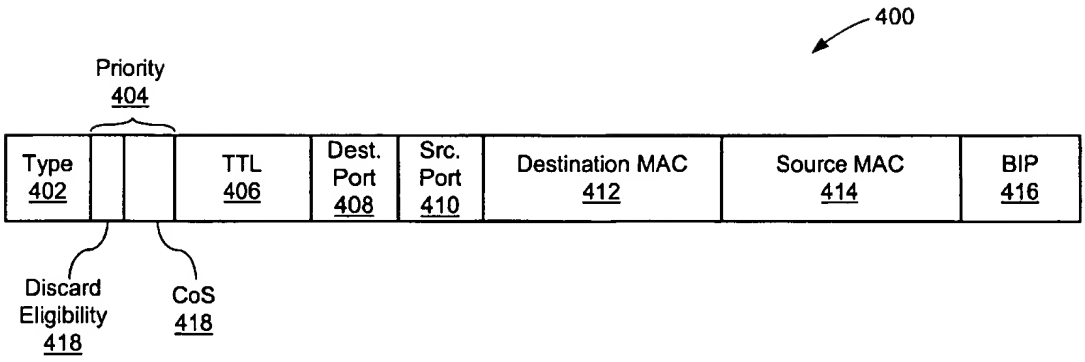
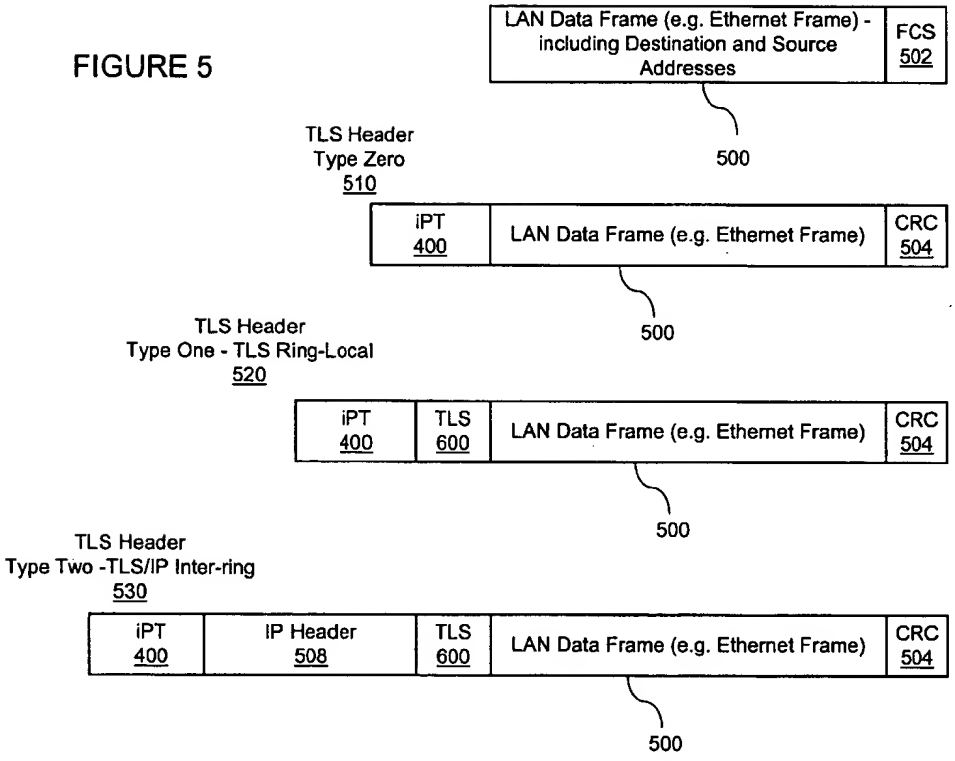

400
Priority
404
Type
402
TTL
406
Dest.
Port
408
Src.
Port
410
Destination MAC
412
Source MAC
414
BIP
416
Discard
Eligibility
418
CoS
418

FIGURE 4

FIGURE 5


LAN Data Frame (e.g. Ethernet Frame) - including Destination and Source Addresses
FCS 502
500
TLS Header Type Zero 510
iPT 400
LAN Data Frame (e.g. Ethernet Frame)
CRC 504
500
TLS Header Type One - TLS Ring-Local 520
iPT 400
TLS 600
LAN Data Frame (e.g. Ethernet Frame)
CRC 504
500
TLS Header Type Two -TLS/IP Inter-ring 530
iPT 400
IP Header 508
TLS 600
LAN Data Frame (e.g. Ethernet Frame)
CRC 504
500

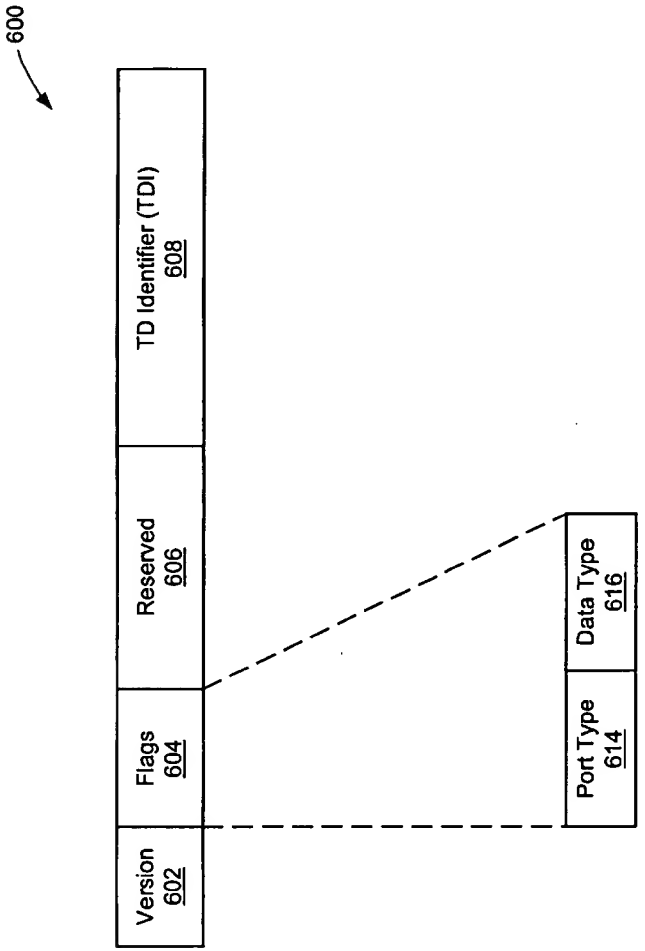


FIGURE 6

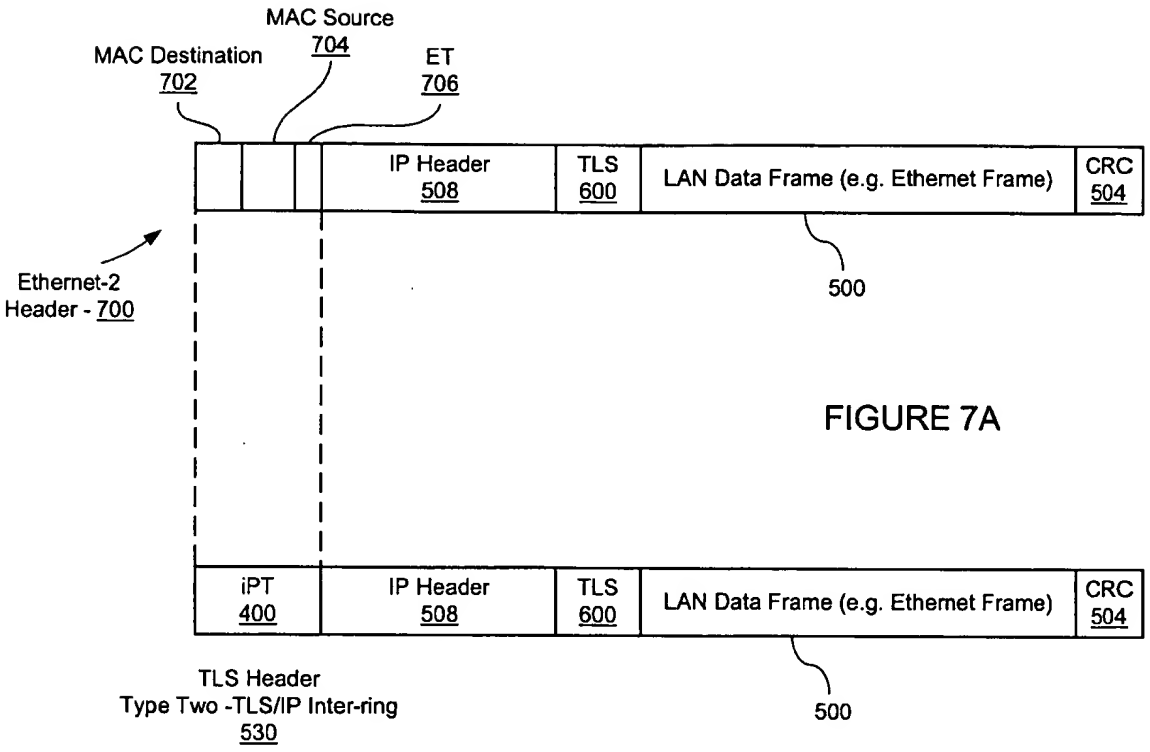

MAC Source
704
MAC Destination
702
ET
706
IP Header
508
TLS
600
LAN Data Frame (e.g. Ethernet Frame)
CRC
504
Ethernet-2
Header - 700
500
iPT
400
IP Header
508
TLS
600
LAN Data Frame (e.g. Ethernet Frame)
CRC
504
TLS Header
Type Two -TLS/IP Inter-ring
530
500

FIGURE 7A

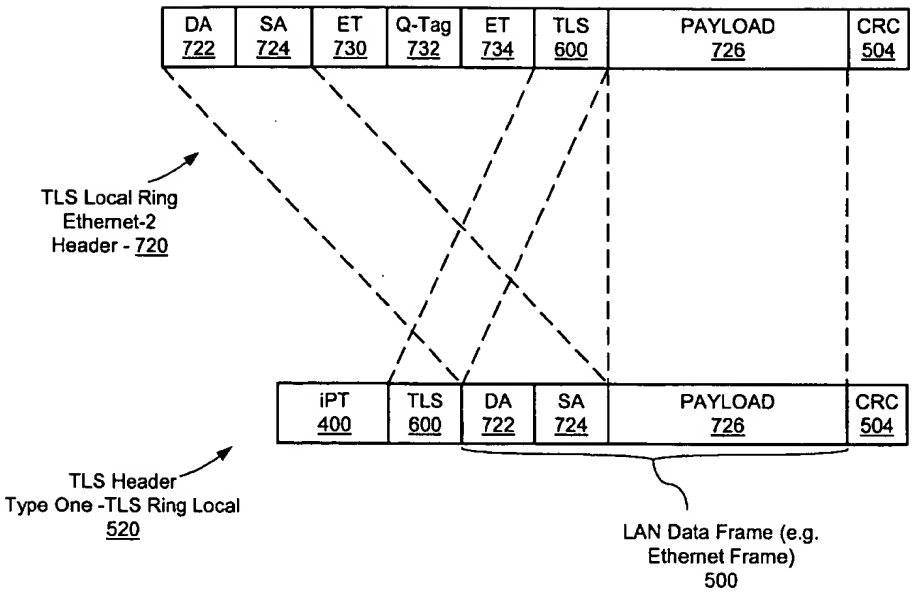

DA 722
SA 724
ET 730
Q-Tag 732
ET 734
TLS 600
PAYLOAD 726
CRC 504
TLS Local Ring Ethernet-2 Header - 720
iPT 400
TLS 600
DA 722
SA 724
PAYLOAD 726
CRC 504
TLS Header Type One -TLS Ring Local 520
LAN Data Frame (e.g. Ethernet Frame) 500

FIGURE 7B

VIRTUAL PRIVATE NETWORKS AND METHODS FOR THEIR OPERATION

REFERENCE TO RELATED APPLICATIONS

This is a continuation in part application of application Ser. No. 09/475,042 (now No. 60/183,049) filed Dec. 30, 1999, and is a continuation in part application of application Ser. No. 09/270,733 filed Mar. 16, 1999, both entitled "Virtual Private Networks and Methods for their Operation" the contents of which are hereby incorporated herein.

FIELD OF THE INVENTION

This invention relates to Virtual Private Networks (VPNs) and methods of their operation. More particularly, this invention relates to methods and apparatus enabling Network Service Providers (NSPs) to provide virtual local area networks (VLANs) services to groups of customers.

BACKGROUND TO THE INVENTION

Transparent LAN Service (TLS) is a data service offered by carriers (such as Bell™ Canada, AT&T™ and MCIWORLDCOM™) today through equipment provided by a variety of manufacturers (such as, for example, Nortel Networks™). The TLS provides native LAN connectivity between several LANs at geographically dispersed sites. The demand for TLS is growing rapidly.

A TLS is typically offered in a metropolitan area including neighboring municipalities. The service and the network to provide the service can be characterized as a virtual private networking service. An individual customer's transparent LAN or VPN, comprised of many LAN sites dispersed across a geographical area, must be secure and separated from other customer's transparent LANs. A customer's sites scattered across a metro area are linked together by the TLS forming a VPN—a group of interconnected LANs that appears to the user as a single, co-located LAN—and are isolated from other VPNs provided by the TLS carrier.

Typically a user's interface to a Transparent LAN Service is a conventional LAN networking protocol such as, for example, Ethernet. TLS is transparent in that the customer appears to access to its own networking media (such as Ethernet) when in reality the media is a shared network with mechanisms to separate the traffic from different VPNs.

Many conventional implementations of the TLS service have been provided using a connection oriented approach. This connection oriented approach typically involves the use of Asynchronous Transfer Mode (ATM) service access Multiplexers (MUXes), ATM switches and Synchronous Optical Network (SONET) add/drop multiplexers (ADMs). However, this connection oriented approach encounters severe scaling problems due, in part, to Permanent Virtual Circuit (PVC) proliferation. Provisioning a fully associated or meshed connection oriented network (that is each node, such as a LAN, is able to communicate with each other node or LAN in the VPN) results in a significant increase in the number of connections, such as PVCs. Moreover, typical PVCs are provisioned to a customer based on a customer's maximum bandwidth requirement. However, since data traffic is typically "bursty" and the dedicated circuits or connections typically provide a fixed bandwidth, the dedicated connections are frequently operating below capacity.

Moreover, the EEE 802.1 standard, the contents of which are hereby incorporated herein, defines a protocol that enables an Ethernet LAN to be partitioned in multiple virtual LANs (VLANs) through the use of a VLAN tag carried in the header of each frame of data. The VLAN tag identifies the VLAN for which the data frame is intended. However, this VLAN tag, defined in the IEEE 802.1 standard as having a twelve bit capacity, limits the number of distinct VLANs, that a carrier, also known as a Network Service Provider (NSP), can accommodate to 4095 (2^{12}–1) VLANs.

Accordingly, a TLS service that enables a carrier to support many (i.e., more than 4095) Virtual Private Networks (VPNs) and a TLS which is scalable and easy to administer is desired.

SUMMARY OF THE INVENTION

A method and an apparatus is disclosed providing Virtual Private Networks (VPNs) to be provisioned over a connectionless network. The method and apparatus provides for a large number VPNs to be provisioned (at least 2^{24} VPNs and as many as approximately 2^{40} VPNs).

Conventional LAN data frames (such as Ethernet frames) are received by an apparatus (an interWAN Packet Transport—iPT card) embodying one aspect of the invention. This receiving or "ingress" iPT card connects a conventional LAN to a wide area transport media such as, for example, a SONET network. Each LAN data frame received will include a destination address of the ultimate destination (for example, a destination media access control—MAC—address, which is a hardware level address that uniquely identifies each node in a network). Based on the destination address incorporated in the LAN data frame, the iPT card will attempt to retrieve address information corresponding to an "egress" iPT card from a stored database (the egress iPT card being connected to the LAN including the ultimate destination). If the ingress iPT card's database has such information, then the LAN data frame is encapsulated in a packet including the retrieved address information. If the egress iPT card is connected to the same transport media as the ingress iPT card (e.g., the iPT cards are connected to the same SONET ring), the address information may include a destination MAC address for the egress iPT card. If the egress iPT is not connected to the same transport media as the ingress iPT card (e.g., the two iPT cards are connected to separate SONET rings), the address information may also contain a secondary destination address such as, for example, an Internet Protocol (IP) address in addition to the other information (e.g., the MAC address of the egress iPT card). The encapsulated LAN data frame will then be routed to the egress iPT card and then to its ultimate destination.

In the event that the ingress iPT card does not include an entry corresponding to the address specified in the destination address portion of the received LAN data frame, a multicast address will be used to encapsulate the received LAN data frame. These multicast encapsulated data frames are then transmitted to all egress iPT cards servicing the particular VPN.

On receipt of an encapsulated LAN data frame, an egress iPT card strips off the header portion, thereby regenerating the original LAN data frame, and forwards this regenerated LAN data frame to its ultimate destination. The header stripped from the encapsulated LAN data frame received by the egress iPT card is then used to populate the egress iPT card's database. This database uses the address information of the source of the LAN data frame (i.e., the source address of the original sending entity and the address information of the ingress iPT card) for LAN data frames received by the egress iPT card for transmission to another iPT card.

According to one aspect of the invention, there is provided a system of providing communication between a first

and a second Local Area Network (LAN), the first and second LANs interconnected by a connectionless network, the system comprising: a first network interface connecting the first LAN to the connectionless network, the first receiving device for: receiving conventional LAN data frames; determining an address of a second network interface responsive to destination information in the received conventional LAN data frames, the second network interface connecting the second LAN to the connectionless network; and encapsulating the conventional LAN data frames received at the first network interface with the address of the second network interface; a router for routing the conventional LAN data frames encapsulated with the address to the second network interface over the connectionless network; the second network interface connecting the second LAN to the connectionless network, the second network interface for: receiving conventional LAN data frames encapsulated with the address; re-generating the conventional LAN data frames from the conventional LAN data frames encapsulated with the address; and transmitting the re-generated conventional LAN data frames to the second LAN; and wherein the determining comprises: determining an identifier uniquely identifying a virtual private network (VPN) comprising at least the first and second LANs; accessing a routing table stored at the first network interface; where possible, retrieving, from the routing table a unique address of the second network interface responsive to a destination address stored in the received LAN data frames and the determined identifier, the unique address comprising an EP address; and if the routing table does not contain the unique address for the destination information, retrieving a multicast address, the multicast address representative of all LANs forming part of the VPN and comprises an IP multicast address; and wherein the encapsulating comprises encapsulating the conventional LAN data frames with the determined identifier and one of the unique address of the second network interface and the multicast address.

According to one aspect of the invention, there is provided a device providing communication between a first and a second Local Area Network (LAN), the first and second LANs in communication by a connectionless network, the device comprising: an input interface in communication with the first LAN; an output interface in communication with the connectionless network; a storage media storing data frames received from the first LAN received via the input interface, data packets and frames for transmission to the second LAN through the output interface; and a processor, the processor adapted to: receive conventional LAN data frames received from the first LAN through the input interface, the received data frames destined for the second LAN; determine, responsive to the received conventional LAN data frames, routing information for routing the received conventional LAN data frames to the second LAN, the routing information comprising an Internet Protocol (IP) address; encapsulate the received conventional LAN data frames with the routing information; transmit the encapsulated conventional LAN data frames to the connectionless network over the output interface; receive encapsulated conventional LAN data frames from the connectionless network from the output interface; generate conventional LAN data frames from the received encapsulated conventional LAN data frames; and transmit the generated conventional LAN data frames to the first LAN by the input interface.

According to one aspect of the invention, there is provided a method of transmitting conventional Local Area Network (LAN) data frames from a first to a second LAN, the first and second LAN interconnected by a connectionless medium, the method comprising: receiving the conventional LAN data frames from the first LAN destined for the second LAN; determining, responsive to the received conventional LAN data frames, routing information for transmittal of the conventional LAN data frames to the second LAN; encapsulating the received conventional LAN data frames with the routing information; transmitting the encapsulated received conventional LAN data frames to the connectionless medium; receiving encapsulated conventional LAN data frames from the connectionless medium destined for the first LAN; generating conventional LAN data frames responsive to the received encapsulated conventional LAN data frames; and transmitting the generated conventional LAN data frames to the first LAN; wherein the determining routing information comprises: determining an identifier uniquely identifying a VPN comprising the first LAN and second LAN; determining from the received conventional LAN data frames the destination for the received conventional LAN data frames; and retrieving, from a database and responsive to the determined destination, an Internet Protocol (IP) address of an egress location forming part of the connectionless medium servicing the determined destination, if the database does not contain an entry for the determined destination, the retrieved address comprising an IP multicast address comprising egress locations servicing the VPN.

According to one aspect of the invention, there is provided a method for facilitating communication in a virtual private network (VPN), the VPN comprising a plurality of local area networks (LANs) each interconnected through a network interface to a connectionless network, comprising, at a first network interface of a first LAN of the VPN: receiving conventional LAN data frames on the first LAN, the conventional LAN data frames having destination information; determining an identifier uniquely identifying the VPN; searching a routing table with the destination information and the identifier for a unique IP address of another network interface of another LAN of the VPN; if the routing table does not contain the unique address, retrieving a multicast IP address for all network interfaces of the plurality of LANs of the VPN; encapsulating the conventional LAN data frames with the identifier and one of the unique IP address and the multicast IP address; and transmitting the encapsulated frames on the connectionless network.

According to one aspect of the invention, there is provided a first network interface for a first local area network (LAN) of a virtual private network (VPN), the VPN comprising a plurality of LANs each interconnected through a network interface to a connectionless network, comprising: means for receiving conventional LAN data frames on the first LAN, the conventional LAN data frames having destination information; means for determining an identifier uniquely identifying the VPN; means for searching a routing table with the destination information and the identifier for a unique address of another network interface of another LAN of the VPN, the unique address comprising an EP address of the another network interface; means for, if the routing table does not contain the unique address, retrieving a multicast address for all network interfaces of the plurality of LANs of the VPN, the multicast address for the all network interfaces comprising a multicast IP address; means for encapsulating the conventional LAN data frames with the identifier and one of the unique address and the multicast address; and means for transmitting the encapsulated frames on the connectionless network.

According to one aspect of the invention, there is provided a Virtual Private Network (VPN) data signal embod-

ied on a carrier wave, the VPN data signal generated from a received conventional LAN data frame, the conventional LAN data frame comprising a LAN destination address, a LAN source address, a LAN payload and a LAN error checking portion, the VPN data signal comprising: an egress destination address of an egress network interface, the egress network interface servicing an egress destination corresponding to the LAN destination address and wherein the egress destination address comprises an Internet Protocol (IP) address; an ingress source address of an ingress network interface, the ingress network interface servicing an ingress source corresponding to the LAN source address and wherein the ingress source address comprises an IP address; the LAN destination address; the LAN source address; the LAN payload; and an error checking portion generated from the egress destination address, the ingress source address, the LAN destination address; and the LAN source address and the LAN payload.

According to one aspect of the invention, there is provided a system of providing communication between a first and a second Local Area Network (LAN), the first and second LANs interconnected by a connectionless network, the system comprising: a first network interface connecting the first LAN to the connectionless network, the first receiving device for: receiving conventional LAN data frames; determining an address of a second network interface responsive to destination information in the received conventional LAN data frames, the second network interface connecting the second LAN to the connectionless network; and encapsulating the conventional LAN data frames received at the first network interface with the address of the second network interface; a router for routing the conventional LAN data frames encapsulated with the address to the second network interface over the connectionless network; the second network interface connecting the second LAN to the connectionless network, the second network interface for: receiving conventional LAN data frames encapsulated with the address; re-generating the conventional LAN data frames from the conventional LAN data frames encapsulated with the address; and transmitting the re-generated conventional LAN data frames to the second LAN; and wherein the determining an address comprises: determining an identifier uniquely identifying a virtual private network (VPN) comprising at least the first and second LANs; accessing a routing table stored at the first network interface; where possible, retrieving, from the routing table a unique address of the second network interface responsive to a destination address stored in the received LAN data frames and the determined identifier; and if the routing table does not contain the unique address for the destination information, retrieving a multicast address, the multicast address representative of all LANs forming part of the VPN and comprises an IP multicast address; and wherein the encapsulating comprises encapsulating the conventional LAN data frames with the determined identifier and one of the unique address of the second network interface and the multicast address; and wherein the routing comprises: receiving the encapsulated conventional LAN data frames at a first Network Network Interface (NNI) of the router; modifying the encapsulated conventional LAN data frames to have a conventional LAN data frame header and LAN data frame payload, the modified encapsulated conventional LAN data frame recognizable by a conventional routing switch of the router; routing, by the routing switch, the modified encapsulated LAN data frame to a second NNI of the router; generating, at the second NNI, an encapsulated conventional LAN data frame from the modified encapsulated data LAN data frame; and transmitting the generated encapsulated conventional LAN data frame to the second network interface.

Other aspects and features of the present invention will become apparent to those ordinarily skilled in the art upon review of the following description of specific embodiments of the invention in conjunction with the accompanying figures.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be more clearly understood after reference to the following detailed specification read in conjunction with the drawings wherein:

FIG. **1** is a schematic of a Transparent LAN Service network;

FIG. **2A** is a schematic of a portion of the TLS network of FIG. **1**;

FIG. **2B** is a detailed schematic of a portion of the network of FIG. **2A**;

FIG. **3** is a detailed schematic of a portion of FIG. **2A**;

FIG. **4** is a data structure embodying one aspect of the present invention and used in the network of FIG. **1**;

FIG. **5** is a schematic of data structures embodying additional aspects of the present invention and used in the network of FIG. **2A**;

FIG. **6** is a schematic of a data structure forming part of some of the data structures of FIG. **5**;

FIG. **7A** is a schematic of a data structure embodying an aspect of the present invention and used in the network of FIG. **2B**; and

FIG. **7B** is a schematic of a data structure embodying an aspect of the present invention and used in the network portion of FIG. **2B**.

DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. **1** illustrates an interWAN Packet Network (iPN) **10**, that embodies one aspect of the instant invention. iPN **10** provides TLS to a plurality of customers (two as illustrated in FIG. **1**). iPN **10** provides communication between a first customer's VPN **12** comprising a plurality of LANs that are typically dispersed across a large geographical area. The communication between LANs comprising VPN **12** is private, or separated from, the communication between a second customer's VPN **14** which is also comprised of a plurality of separated LANs.

iPN **10** is a connectionless network, such as an Internet Protocol (IP) network. That is, no hard-wired or virtual connections exist between any two points, such as the LANs comprising VPNs **12** or **14**, nor are these connections provided by iPN **10**. Rather data packets or frames are individually and dynamically routed from a source to a destination through the packet switches forming iPN **10**.

The present invention is designed to accommodate the desire for customers to have their LANs communicate over relatively small geographical areas, such as a metropolitan area, or much larger geographical areas, such as an entire country or even larger areas.

FIG. **2A** illustrates in greater detail a first embodiment of the iPN **10**. iPN **10** comprises a plurality of VPNs **12**, **14** and **16** interconnected through a plurality of local rings **22A**, **22B** and **22C** (collectively local rings **22**). Local rings **22** inter-communicate through inter-ring **20**. Local rings **22** and inter-ring **20** may be, for example, a SONET network or

other network type that is capable of carrying the data packets described herein. As will be appreciated by those skilled in the art, local rings **22A**, **22B** and **22C** are only exemplary and the TLS described herein may be implemented over other network types capable of carrying data packets such as, for example, Ethernet frames or IP frames, as long as the User-Network Interface (UNI) and Network-Network Interface (NNI) functions described herein are implemented on a network element(s) forming part of a network.

The embodiment illustrated in FIG. **2A** has VPN **16** comprised of three LANs in communication with local ring **22C**, VPN **14** comprising three LANs—two in communication with local ring **22B** and the third in communication with local ring **22A**, and VPN **12** comprising five LANs—two in communication with local ring **22A**, two in communication local ring **22B** and the last LAN in communication with local ring **22C**. The LANs comprising VPNs **12**, **14** and **16** transmit to and receive data from local rings **22** through multiplexers **24** equipped with both: (1) LAN networking protocol interfaces, such as Ethernet interfaces; and (2) a packet switching interface. Multiplexers **24**, hereinafter referred to as interWAN Packet Transport (iPT) cards **24**, may be, for example, modified SONET ADMs. The modifications, which implement the methods and apparatus described herein, may include hardware and/or software modifications to conventional SONET ADMs. Local rings **22** communicate with inter-ring **20** through central offices (CO) **18A** and **18B** (collectively COs **18**). COs **18** incorporate routing switches, such as, for example, Ethernet or IP routing switches, to route packets transmitted between local rings **22**.

An exemplary CO **18** is illustrated in greater detail in FIG. **2B**. CO **18** comprises a first NNI **200** in communication with a conventional routing switch **204**. Routing switch **204** is also in communication with a second NNI **202**. First and second NNIs **200**, **202** perform functions described herein and are each in communication with a ring **22** or inter-ring **20**.

VPN **16**, which comprises three LANs all in communication with a single local ring **22C**, can be described as operating as a local ring TLS. VPNs **12** and **14**, which, as described below, operate as a TLS/IP inter-ring TLS.

Generally, and described in greater detail below, a VPN and a broader TLS implemented in accordance with the invention disclosed herein can operate as a local ring TLS, which provides for local bridging when all of the LANs comprising the VPN are in communication with a single local ring **22**, or the VPN can operate as a TLS/IP inter-ring VPN which provides an inter-ring solution with improved scaling properties when compared to a connection oriented transparent LAN service. As the name implies, a TLS/IP implementation of the present invention uses the internet protocol (IP) together with IP Learning Tunnels (IPLT) described hereinafter. Using IP leverages the inherent scalability of IP routing by using an IP routed network backbone for iPN **10**. The present invention uses IP encapsulation and IP routing and multicasting to encapsulate layer two (L2) traffic over an EP network. Further, using the dynamic learning technique, described as IPLT, ensures traffic from separate VPNs, such as VPNs **12**, **14** and **16**, is kept separate from each other thus providing the "private" aspect of a VPN. Moreover, the IPLT technique offers simple provisioning by dynamically creating routing tables based on traffic flow and provides efficient use of the bandwidth provided by a local ring **22** or an inter-ring **20**.

Accordingly, a TLS is provided by iPN **10** by providing the capability to separate and transport customer data frames, such as Ethernet frames, across a shared network, such as iPN **10**. A customer's data frames (hereinafter referred to as Ethernet frames for simplicity although other networking protocols can also be used) are encapsulated and routed over the IP backbone between the various LANs that comprise the VPN. Consequently, a user can subscribe to a VPN offered by a carrier's TLS implementing the present invention to connect all its different physical sites into an apparently single LAN (as viewed by the customer). Alternatively, a customer may subscribe to a VPN offered by a carrier's TLS to transport traffic between selected sites or, if desired, a group of separate customers, such as a plurality of suppliers and their customer(s), may subscribe to form a single VPN connecting these different organizations.

Each of a customer's LANs will be connected to local ring, such as a local ring **22** which may be, for example, a SONET ring. The LANs will connect to a local ring through an iPT card **24**. Each iPT card can have a plurality of virtual ports, such as Ethernet ports, mapping on to a plurality of physical ports. Each TLS virtual port on the iPT card can be individually configured to operate as a User-Network Interface (UNI) port—an interface between a customer's LAN and a local ring—or a Network-Network Interface (NNI) port—a port used to interconnect separate rings (e.g., local rings **22** or inter-ring **20**).

In operation and without limiting the subsequent description contained herein, a UNI port may be dedicated to a particular customer and a particular customer's LAN. Each UNI port will be configured with a unique address (e.g., an IP address), which provides a unique address for the virtual port on that particular VPN. Moreover, each iPT card **24** will be provisioned with a unique address (e.g., an EP address). Each VPN will be assigned a unique TLS Domain (TD) identifier (TDI). Accordingly, every UNI port forming part of a single VPN or TLS domain will use the same TDI. Therefore, a LAN forming part of a VPN can be identified by the IP address of its associated iPT card **24** and the address for the UNI port of the card servicing the LAN. Further, the entire VPN will be identified on iPN **10** (FIG. **1**) by a unique TDI. Finally, each TD will also be associated with a multicast group address which will be used to multicast a message to the entire domain. As described in greater detail below, the multicast group address will take either the form of an EP multicast group address when the VPN has member LANs connected to a plurality of local rings (i.e., the VPN operates as an inter-ring VPN) or a TLS local ring multicast group address (i.e., the VPN operates as a local ring VPN). A multicast group address (i.e., either an EP or TLS multicast address) will be used during the dynamic learning of addresses of other members of a TD. It may be desirable to map a multicast group address directly to its associated TDI (i.e., the multicast group address maps 1:1 to the TDI for a particular TD). It should also be noted that since iPT cards **24** form part of their associated LANs, each iPT card will, like all other networked devices on a LAN, have a unique Media Access Control (MAC) address. As is known by those skilled in the art, a MAC address is a hardware level forty-eight bit address that uniquely identifies each node in a network.

An IP multicast group address is used in the circumstance where the sending entity (i.e., the sending device forming part of the source LAN) desires to transmit data to a second entity having a MAC address that may be known by the sending entity and a unicast IP address which is unknown to the sending iPT card and the sending entity forms part of a given inter-ring VPN.

In the above-noted circumstance (i.e., an unknown unicast IP address), the sending customer transmits Ethernet frames